

Exhibit 2

US8677116B1	American Airline's website "aa.com" ("The accused instrumentality")
1. A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:	<p>The accused instrumentality practices a method of using a computer system (e.g., authentication server of the accused instrumentality, etc.) to authenticate a user seeking to conduct at least one interaction (e.g., account login, etc.) with a secured capability provided by a computer (e.g., server of the accused instrumentality).</p> <p>As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, job searches, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access.</p>

The screenshot shows the American Airlines website homepage. At the top, there is a navigation bar with links for "Plan travel", "Travel information", "AAdvantage®", "Log in", and "Join". A search bar is also present. A promotional banner in the center of the page says "Earn 50,000 bonus miles" and includes a smaller text: "Plus, first checked bag is free on domestic American Airlines itineraries". Below the banner, there is a photo of two people in a boat on a lake. A Citi AAdvantage credit card is shown in the bottom right corner of the banner. Below the banner, there are three tabs: "Book", "Manage trips / Check-in", and "Flight status". The "Book" tab is selected. Underneath, there are dropdown menus for "Flights" (selected) and "Vacations", and buttons for "Round trip" and "1 passenger". Below these are input fields for "From" (BOM), "To" (Going to), "Depart" (mm/dd/yyyy), and "Return" (mm/dd/yyyy). A "Search" button is located at the bottom right of the search area.

<https://www.aa.com/homePage.do>

American Airlines 

PLAN TRAVEL TRAVEL INFORMATION AADVANTAGE® 

[Log in](#)

You can log in with your AAdvantage number or username and password.

[Join AAdvantage today »](#)

(* Required)

AAdvantage # or username * Password * 

Remember me

[Need help logging in? !\[\]\(760156e5f29de4babee4bb59dd060835_img.jpg\)](#)

<https://www.aa.com/loyalty/login>

The screenshot shows the homepage of AA.com. At the top left is the American Airlines logo. To the right are links for "Plan travel", "Travel information", "AAdvantage®", and a "Log In" button. A search bar with the placeholder "Search AA.com®" and a magnifying glass icon is located at the top right. Below the header is a large, light gray rectangular area labeled "Banner". In the center of the page, a red-bordered box contains the greeting "Hi PRASAD, welcome to the AAdvantage® program!". At the bottom of the page, there are two hyperlinks: "<https://www.aa.com/loyalty/login>" and "<https://www.aa.com/homePage.do>".

A screenshot of a web browser window showing the URL "aa.com/homePage.do" in the address bar. A context menu is open over the address bar, with the "Connection is secure" option highlighted by a red box. Other menu items include "Cookies and site data", "Ad privacy", and "Site settings". The background of the browser shows the American Airlines homepage with its signature blue and white color scheme and a mountain landscape image.

The screenshot shows a browser's security panel on the left and a detailed security overview on the right. The security panel includes sections for Main origin and Secure origins, with a link to <https://ingest.quantumme.com>. The security overview panel displays a green lock icon and the message "This page is secure (valid HTTPS)". A red box highlights this message. Below it, three items are listed: "Certificate - valid and trusted", "Connection - secure connection settings", and "Resources - all served securely".

<https://www.aa.com/homePage.do>

Request Headers

POST /fb_bf04553ytd?type=js&sn=v_4_srv_3_sn_97858845F626016C22C90F2A94A0CC91_perc_100000_oI_0_mul_1_app-3A8b2a7e

Content-Type: text/plain; charset=UTF-8

Miscellaneous

Referer: https://www.aa.com/homePage.do

Security

Origin: https://www.aa.com
 sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A_Brand";v="24"
 sec-ch-ua-mobile: ?0
 sec-ch-ua-platform: "Windows"
 Sec-Fetch-Dest: empty
 Sec-Fetch-Mode: no-cors
 Sec-Fetch-Site: same-origin

Transport

Source: Fiddler capture of the accused instrumentality

Name	Value	Do...	Path	Expires / Max-Age	Size	HttpO...	Secure	SameSite	Partition...	Cross Site	Priority
JSESSIONID	DAEBAEA330F6DF9CDE1B18FA5FC70...	w...	/	Session	42	✓	✓				Medium
KROUTEID	eb7a9eaf63cea5a7af6a1b26cd4081e8...	w...	/	Session	73	✓	✓				Medium
OPT0492	B_OPT0492_Exp hp-booking-widget[2]...	w...	/	Session	98		✓				Medium
OPTCKMS	n	.aa...	/	2025-02-20T06:51:43.000Z	8						Medium
OPTOUTMULTI	0:0%7Cc1:0%7Cc3:0	.aa...	/	2025-02-20T06:51:43.000Z	28						Medium
OPTOUTMULTI_EXP	Thu, 20 Feb 2025 06:51:43 GMT	.aa...	/	2025-02-20T06:51:43.000Z	44						Medium
QSI_HistorySession	https%3A%2F%2Fwww.aa.com%2Floy...	w...	/	Session	129		✓				Medium
QuantumMetricSessionID	2c92a8004d61ab9e00a4a2eab9802b5c	.aa...	/	2024-11-22T10:26:55.000Z	54		✓	None			Medium
QuantumMetricUserID	d85681e5345f547b026967123e4f170a	.aa...	/	2025-11-22T09:44:35.000Z	51		✓	None			Medium
ROUTEID	IKSS.blue	w...	/	2024-11-22T10:13:02.030Z	16						Medium
RT	"z=1&dm=www.aa.com&si=c36703a...	w...	/	2024-11-29T09:44:31.000Z	95			Lax			Medium
TDCPM	CAESFgoHnViaWNvbhlCKagy-aX8...	ad...	/	2025-11-22T09:44:33.070Z	797		✓	None			Medium
TDID	c68ea1d-9b3f-4a9e-b2aa-e0bfae3b...	ad...	/	2025-11-22T09:44:33.070Z	40		✓	None			Medium
TL540H50	0	w...	/	2025-02-20T06:51:43.000Z	9						Medium
UAC	143ddd3a7158451186e7ab4eadc6ed7e	w...	/	2025-12-27T06:51:42.204Z	35		✓				Medium
X-AK-PIM-INJECT	sync	w...	/	Session	19						Medium
X-ANPDR-PAIRID	EE61-G1CE-INVHNU-2NKK-5-HL4		/	2025-02-20T09:44:33.120Z	140						Medium

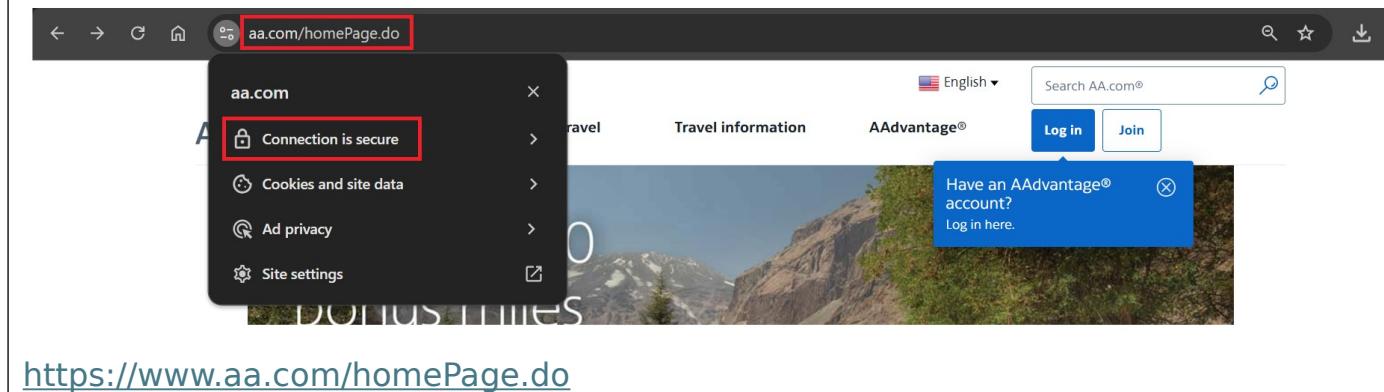
<https://www.aa.com/homePage.do>

using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;

The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a first signal (e.g., a ROUTEID set response, etc.) from the computer (e.g., server of the accused instrumentality) providing the secured capability (e.g., secure connection with the website, etc.), the first signal comprising a reusable identifier (e.g., ROUTEID, etc.) corresponding to the secured capability (e.g., secure connection with the website, etc.), the reusable identifier assigned for use by the secured capability for a finite period of time (e.g., Max-Age).

As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. The server sends a response to set ROUTEID value, which is set by the user device.

As shown, the ROUTEID token set by the end device is reused in all further communications with the server. The ROUTEID token also mentions a Max-Age for the token, indicating that it can be reused for a finite period.



The screenshot shows a browser's security panel on the left and a detailed security overview on the right. The security panel includes sections for Main origin and Secure origins, with a link to <https://ingest.quantumme.com>. The security overview panel displays a green lock icon and the message "This page is secure (valid HTTPS)". A red box highlights this message. Below it, three items are listed: "Certificate - valid and trusted", "Connection - secure connection settings", and "Resources - all served securely".

<https://www.aa.com/homePage.do>

The image shows two screenshots from Fiddler, a network traffic debugger.

Screenshot 1 (Top): Security View

- Origin: https://www.aa.com
- sec-ch-ua: Google Chrome ;v="131", "Chromium";v="131", "Not_A_Brand";v="24"
- sec-ch-ua-mobile: ?0
- Receive a first signal from the computer
- Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies
- Raw JSON XML
- Response sent 36 bytes of Cookie data:
- Set-Cookie: ROUTEID=IKSS.blue;Path=/;Max-Age=960

A red box highlights the "Set-Cookie" line, and a red arrow points from it to the text "Finite period of time".

Screenshot 2 (Bottom): Cookies Table

Name	Value	Do...	Path	Expires / Max-Age	Size	HttpO...	Secure	SameSite	Partition...	Cross Site	Priority
JSESSIONID	DAEBAEA330F6DF9CDE1B18FA5FC70...	w...	/	Session	42	✓	✓				Medium
KROUTEID	eb7a9eaf63cea5a7af6a1b26cd4081e8...	w...	/	Session	73	✓	✓				Medium
OPT0492	B_OPT0492_Exp hp-booking-widget 2...	w...	/	Session	98		✓				Medium
OPTCKMS	n	.aa...	/	2025-02-20T06:51:43.000Z	8						Medium
OPTOUTMULTI	0:0%6Cc10%6Cc3:0	.aa...	/	2025-02-20T06:51:43.000Z	28						Medium
OPTOUTMULTI_EXP	Thu, 20 Feb 2025 06:51:43 GMT	.aa...	/	2025-02-20T06:51:43.000Z	44						Medium
QSI_HistorySession	https%3A%2F%2Fwww.aa.com%2Floy...	w...	/	Session	129		✓				Medium
QuantumMetricSessionID	2c92a8004d61ab9e00a4a2eab9802b5c	.aa...	/	2024-11-22T10:26:55.000Z	54	✓	✓	None			Medium
QuantumMetricUserID	d85681e5345f547b026967123e4f170a	.aa...	/	2025-11-22T09:44:35.000Z	51	✓	✓	None			Medium
ROUTEID	IKSS.blue	w...	/	2024-11-22T10:13:02.030Z	16						Medium
RT	"z=1&dm=https://www.aa.com&si=3c6703a...	w...	/	2024-11-29T09:44:31.000Z	95			Lax			Medium
TDCPM	CAESFgoHcnViaWNvbhlCKagy-xi8...	ad...	/	2025-11-22T09:44:33.070Z	797	✓	✓	None			Medium
TDID	c68eaa1d-9b3f-4a9e-b2aa-e0bfae3b...	ad...	/	2025-11-22T09:44:33.070Z	40	✓	✓	None			Medium
TL540H50	0	w...	/	2025-02-20T06:51:43.000Z	9						Medium
UAC	143ddd3a7158451186e7ab4eadc6ed7e	w...	/	2025-12-27T06:51:42.204Z	35		✓				Medium
X-AK-PIM-INJECT	sync	w...	/	Session	19						Medium

<https://www.aa.com/homePage.do>

	<p>Request Headers</p> <p>POST /rb_bf04553ytd?type=js3&sn=v_4_srv_3_sn_97858845F626016C22C90F2A94A0CC91_perc_100000_oI_0_mul_1_app-3A8b2a7e OPTOUTMULTI=0:0%7Cc1:0%7Cc3:0 QSI_HistorySession=https%3A%2F%2Fwww.aa.com%2Floyalty%2Fenrollment%2Fenroll%3Ffrom%3Dcomp_nav~17322 QuantumMetricSessionID=2c92a8004d61ab9e00a4a2eab9802b5c QuantumMetricUserID=d85681e5345f547b026967123e4f170a ROUTEID=IKSS.blue Reusable identifier └ RT "z=1 dm=www.aa.com</p>
	<p>Source: Fiddler Capture of the accused instrumentality</p>
	<p>Request Headers</p> <p>GET /AtVvXc/Jsf2GP/UhFxP9/PKeXfrNC/0/QYO56tw1fY1u/cCYfZCEC/ETc0/W3ccDj8 HTTP/1.1 mboxEdgeCluster=41 OPT0492=B_OPT0492_Exp hp-booking-widget 20241111-OPT0492-AB-HP-Booking-Widget-Server-Side-Test-PROD OPTCKMS=n OPTOUTMULTI_EXP=Thu, 20 Feb 2025 06:51:43 GMT OPTOUTMULTI=0:0%7Cc1:0%7Cc3:0 QSI_HistorySession=https%3A%2F%2Fwww.aa.com%2Floyalty%2Fenrollment%2Fenroll%3Ffrom%3Dcomp_nav~17322 QuantumMetricSessionID=2c92a8004d61ab9e00a4a2eab9802b5c QuantumMetricUserID=d85681e5345f547b026967123e4f170a ROUTEID=IKSS.blue Reusable identifier └ RT "z=1 dm=www.aa.com</p>
	<p>Source: Fiddler Capture of the accused instrumentality</p>
using the computer system to receive a	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a second signal

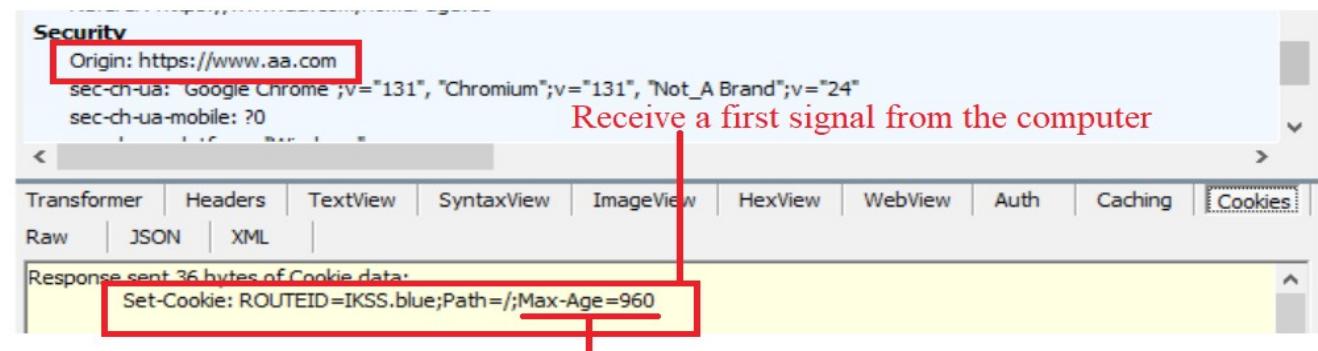
<p>second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information;</p>	<p>(e.g., a request signal from the user device) from an electronic device being used by the user, the second signal (e.g., request signal from the user device) comprising a copy of the reusable identifier (e.g., ROUTEID, etc.) and user verification information (e.g., rxVisitor).</p> <p>When the server sends a message containing an ROUTEID to the user device, the client includes a copy of the ROUTEID in all subsequent requests to the server, along with user verification information (e.g., rxVisitor credentials). This allows the server to authenticate the client for the duration of the session and ensure secure communication between the client and server.</p> <div data-bbox="662 627 2010 960"><p>Request Headers [Raw] [Header Definitions]</p><p>POST /tb_bf04553ytd?type=js3&sn=v_4_srv_3_sn_97858845F626016C22C90F2A94A0CC91_perc_100000_o_l_0_mul_1_app-3A8b2a7e OPTOUTMULTI=0:0%7Cc1:0%7Cc3:0 QSI_HistorySession=https%3A%2Fwww.aa.com%2Floyalty%2Fenrollment%2Fenroll%3Ffrom%3Dcomp_nav~17322 QuantumMetricSessionID=2c92a8004d61ab9e00a4a2eab9802b5c QuantumMetricUserID=d85681e5345f547b026967123e4f170a ROUTEID=IKSS.blue Reusable identifier RT z=1 dm=www.aa.com</p></div> <p>Source: Fiddler Capture of the accused instrumentality</p>
--	--

	<p>Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML </p> <p>Request sent 4161 bytes of Cookie data:</p> <pre>XSRF-TOKEN=1fc611a7-8e0b-43a2-b26e-02e81ff863b9 UAC=143cdd3a7158451186e7ab4eadc6ed7e sessionLocale=en_US aka_state_code=MH aka_cr_code=TN-MH rxVisitor=1732258302690CFU4JCN7O6I7N7NEMUAIHFS5TR9OHC60 at_cneck=true AMCVS_025C69945392449B0A490D4C%40AdobeOrg=1 TL540H50=0 OPTOUTMULTI=0:0%7Cc1:0%7Cc3:0</pre>
	<p>Source: Fiddler capture of the accused instrumentality</p> <p>Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML </p> <pre>_gd_au=1.1.507214269.1732258305 QuantumMetricUserID=d85681e5345f547b026967123e4f170a OPT0492=B_OPT0492_Exp hp-booking-widget 20241111-OPT0492-AB+HP-Booking-Widget-Server-Side-Test-PROD al=0 s_sq=%5B%5B%5D%5D _fbp=fb.1.1732258314476.89935556667487536 QuantumMetricSessionID=2c92a8004d61ab9e00a4a2eb9802b5c KROUTEID=eb7a9eaf63cea5a7af6a1b26cd4081e8 b1f37ed7f54333e7fed5541bf6553ced dtCookie=v_4_srv_3_sn_97858845F626016C22C90F2A94A0CC91_perc_100000_ol_0_mul_1_app- 3A8b2a7e44ceb3fcda4_1_app-3A165a5cc5c5fd7c11_1_rcs-3Acss_0 SESSIONID=CD0FF3D2876F65C771221563762C1685 ROUTEID=IKSS.blue AKA_A2=A mboxEdgeCluster=41 ak_bmsc=</pre>
	<p>Source: Fiddler capture of the accused instrumentality</p> <p>using a processor of the computer system to evaluate, based at least on the first signal (e.g., a ROUTEID set response, etc.) and</p> <p>The accused instrumentality practices using a processor of the computer system (e.g., processor of the authentication server of the accused instrumentality, etc.) to evaluate, based at least on the first signal (e.g., a ROUTEID set response, etc.) and</p>

on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and

the second signal (e.g., a request signal from the user device), whether the user is authorized to conduct the at least one interaction (e.g., account login, etc.) with the secured capability (e.g., secure connection with the website, etc.).

The server compares the reusable identifier, such as the token (e.g., ROUTEID), in the first response received from the server with the token included in the client's subsequent request. If a match is found, the server authenticates the user and processes the request securely.



Source: Fiddler captures of the accused instrumentality

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

Request sent 4161 bytes of Cookie data:

```
XSRF-TOKEN=1fc611a7-8e0b-43a2-b26e-02e81ff863b9
UAC=143ddd3a7158451186e7ab4eadc6ed7e
sessionLocale=en_US
aka_state_code=MH
aka_cr_code=IN-MH
rxVisitor=1732258302690CFU4JCN7O6I7N7NEMUAIHFS5TR9OHC60
at_check=true
AMCVS_025C69945392449B0A490D4C%40AdobeOrg=1
```

Source: Fiddler Capture of the accused instrumentality

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

```
_gd_au=1.1.507214269.1732258305
QuantumMetricUserID=d85681e5345f547b026967123e4f170a
OPT0492=B_OPT0492_Exp|hp-booking-widget|20241111-OPT0492-AB-HP-Booking-Widget-Server-Side-Test-PROD
al=0
s_sq=%5B%5B%5D%5D
_fbp=fb.1.1732258314476.89935556667487536
QuantumMetricSessionID=2c92a8004d61ab9e00a4a2eab9802b5c
KROUTEID=eb7a9eaf63cea5a7af6a1b26cd4081e8|b1f37ed7f54333e7fed5541bf6553ced
dtCookie=v_4_srv_3_sn_97858845F626016C22C90F2A94A0CC91_perc_100000_ol_0_mul_1_app-
3A8b2a7e44ceb3fcfd4_1_app-3A165a5cc5c5fd7c11_1_rcs-3Acss_0
SESSIONID=CD0FF3D2876F65C771221563762C1685
ROUTEID=IKSS.blue
```

the second signal comprising a copy of the reusable identifier

Source: Fiddler capture of the accused instrumentality

The screenshot shows the American Airlines website homepage. At the top, there is a navigation bar with links for "Plan travel", "Travel information", "AAdvantage®", "Log in", and "Join". A search bar is also present. A red box highlights the "American" logo. Below the navigation, a large banner features a scenic mountain landscape with two people in a boat. The banner text reads "Earn 50,000 bonus miles" and "Plus, first checked bag is free on domestic American Airlines itineraries". A small note says "Terms apply". To the right of the banner, a blue button says "Have an AAdvantage® account? Log in here." Below the banner, there are three tabs: "Book", "Manage trips / Check-in", and "Flight status". The "Book" tab is selected and shows options for "Flights" (selected) and "Vacations". It includes fields for "From" (BOM), "To" (Going to), "Depart" (mm/dd/yyyy), "Return" (mm/dd/yyyy), and a "Search" button. A Citi AAdvantage credit card is displayed on the right side of the search area.

<https://www.aa.com/homePage.do>

American Airlines 

PLAN TRAVEL TRAVEL INFORMATION AADVANTAGE® 

[Log in](#)

You can log in with your AAdvantage number or username and password.

[Join AAdvantage today »](#)

(* Required)

AAdvantage # or username * Password * 

Remember me

[Need help logging in? !\[\]\(744ed445582ccec540556169f001c532_img.jpg\)](#)

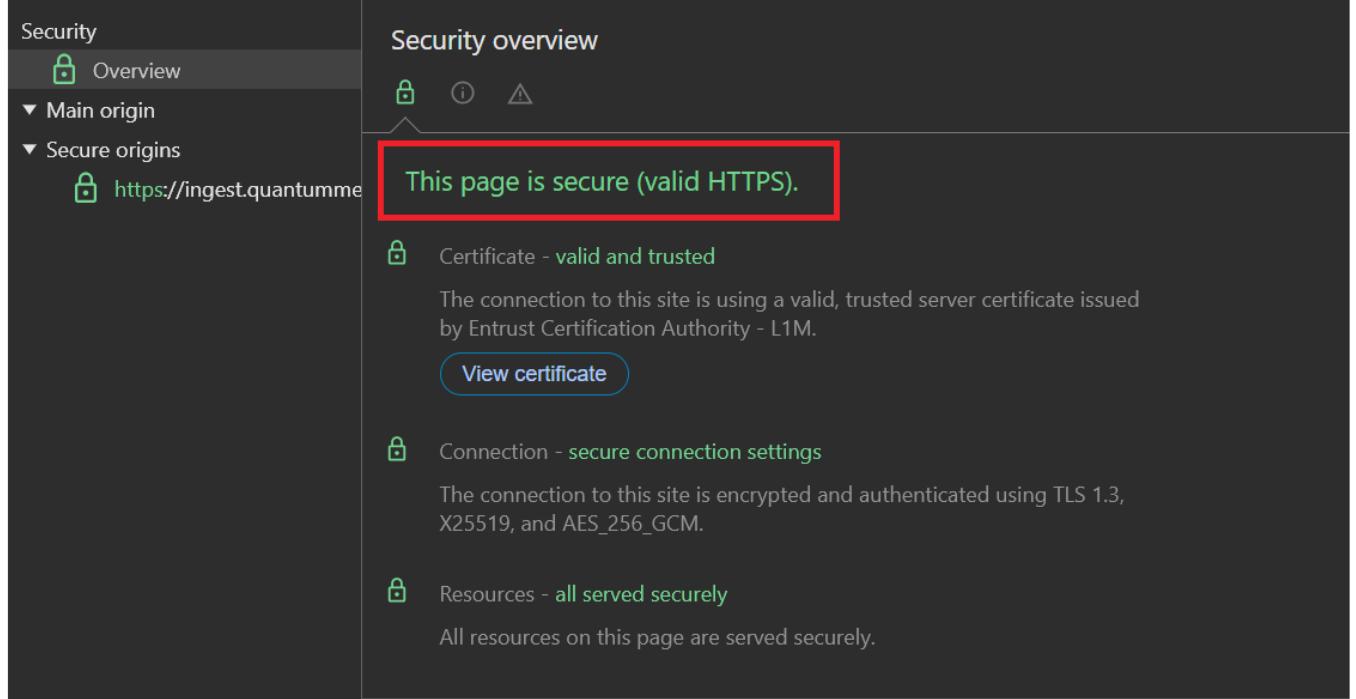
<https://www.aa.com/loyalty/login>

The screenshot shows the American Airlines website (www.aa.com) with a large red box highlighting the "American" logo in the top left corner. The top navigation bar includes links for "Plan travel", "Travel information", "AAdvantage®", and a "Log In" button. A search bar is located in the top right. Below the navigation is a large gray rectangular area labeled "Banner". A red box highlights the greeting "Hi PRASAD, welcome to the AAdvantage® program!".

<https://www.aa.com/loyalty/login>

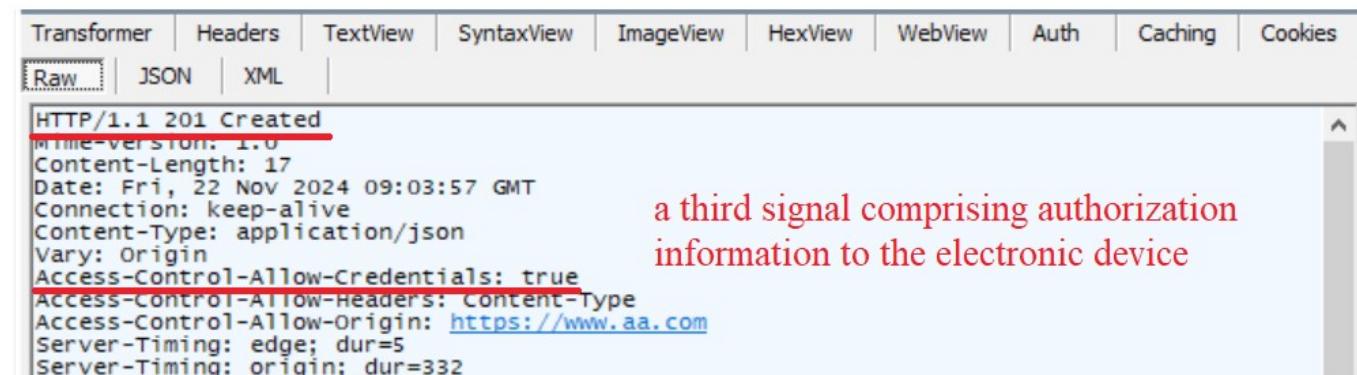
This screenshot shows the same website as above, but with a browser's security information overlay. The address bar shows "aa.com/homePage.do". A dark overlay window displays the message "Connection is secure" next to a padlock icon. Other options in the overlay include "Cookies and site data", "Ad privacy", and "Site settings". The main page content is partially visible behind the overlay.

<https://www.aa.com/homePage.do>

	 <p>https://www.aa.com/homePage.do</p>
in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal	The accused instrumentality practices in response to an indication from the processor (e.g., processor of the authentication server of the accused instrumentality, etc.) that the user is authorized to conduct the at least one interaction with the secured capability (e.g., secure connection with the website, etc.), using the computer system processor (e.g., authentication server of the accused instrumentality, etc.) to transmit a third signal comprising authorization information (e.g., a response signal from the server to the user device, etc.) to at least one of the electronic device (e.g., user device, etc.) and the computer.

comprising authorization information to at least one of the electronic device and the computer.

As shown, upon authenticating the ROUTEID, the user device receives an authentication confirmation message (a third signal), from the server to the user device.



The screenshot shows a Fiddler network traffic capture. The top navigation bar includes Transformer, Headers, TextView, SyntaxView, ImageView, HexView, WebView, Auth, Caching, and Cookies tabs. The Headers tab is selected, showing the following response headers:

Header	Value
HTTP/1.1	201 Created
Content-Type	application/json
Content-Length	17
Date	Fri, 22 Nov 2024 09:03:57 GMT
Connection	keep-alive
Vary	Origin
Access-Control-Allow-Credentials	true
Access-Control-Allow-Headers	Content-Type
Access-Control-Allow-Origin	https://www.aa.com
Server-Timing	edge; dur=5
Server-Timing	origin; dur=332

a third signal comprising authorization information to the electronic device

Source: Fiddler capture of the accused instrumentality

The screenshot shows the American Airlines website homepage. At the top, there is a navigation bar with links for "Plan travel", "Travel information", "AAdvantage®", "Log in", and "Join". A search bar is also present. A promotional banner in the center of the page says "Earn 50,000 bonus miles" and includes a smaller text: "Plus, first checked bag is free on domestic American Airlines itineraries". Below the banner, there is a callout box asking if the user has an AAdvantage account, with "Log in here." and "Join" buttons. A Citi AAdvantage credit card is shown on the right side of the banner. Below the banner, there is a search interface with tabs for "Book", "Manage trips / Check-in", and "Flight status". The "Book" tab is selected, showing options for "Flights" (selected) and "Vacations". Below this, there are fields for "From" (BOM), "To" (Going to), "Depart" (mm/dd/yyyy), and "Return" (mm/dd/yyyy). A "Search" button is located at the bottom right of the search area. The background of the page features a scenic image of two people in a boat on a lake with mountains in the background.

<https://www.aa.com/homePage.do>